AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

Claims 1-41 (Cancelled).

42. (Currently Amended) A combinatorial key-dependent network for encryption/decryption of input digital data having a first word size into output digital data of the same word size, comprising at least two layers, each layer comprising at least an elementary building block, each building block operating on an input block of bits having a second word size smaller than or equal to said first word size, for generating an output block of bits, said building block comprising:

a multiplexer circuit that receives a first portion of said input block of bits and a first set of key bits as inputs, the first portion of said input block of bits operable to select a second set of key bits out of the first set of key bits, wherein the selected second set of key bits are output by said multiplexer circuit, said first portion of bits are transferred intact without modification by an encryption operation to an output of said building block, and the number of bits in the second set of key bits is less than the number of bits in the first set of key bits; and

a transformation circuit, for transforming a second portion of said input block of bits into transformed bits according to a reversible transformation chosen, by means of said selected second set of key bits, among a plurality of reversible transformations implemented in said transformation circuit, wherein said transformation circuit transforms said second portion of said input block of bits without receiving said

first portion of said input block of bits as an input and said output block of bits comprises the transformed bits followed by said first portion of said input block of bits.

43. (Previously Presented) The network according to claim 42, wherein adjacent layers are connected by means of a fixed bit permutation block.

44. (Previously Presented) The network according to claim 43, comprising a plurality of fixed bit permutation blocks of the same type.

45. (Previously Presented) The network according to claim 43, comprising at least two different types of fixed bit permutation blocks.

46. (Previously Presented) The network according to claim 43, wherein bits in said first portion of said input block of bits are used, in a next layer, as bits to be transformed.

47. (Previously Presented) The network according to claim 43, wherein, for each building block, said first portion of said input block of bits are extracted from at least two building blocks in a preceding layer, provided that said first portion of said block of bits comprise at least two bits.

48. (Previously Presented) The network according to claim 43, wherein, for each building block, said second portion of said input block of bits are extracted from at least two building blocks in a preceding layer, provided that said second portion of said block of bits comprises at least two bits.

49. (Previously Presented) The network according to claim 42, wherein each layer comprises at least two building blocks.

50. (Previously Presented) The network according to claim 49, wherein said reversible transformations are such that each output bit of said transformed bits is a non-linear function of said first portion of said input block of bits and of said second set of key bits, with the algebraic normal form containing at least one binary product involving both said second portion of said input block of bits and said second set of key bits.

51. (Previously Presented) The network according to claim 50, wherein said reversible transformations satisfy a criterion that the uncertainty of the second portion of said input block of bits provided by uniformly random second set of key bits when the transformed bits are known is equal to a bit size of the transformed bits.

52. (Previously Presented) The network according to claim 42, wherein said multiplexer circuit comprises a lookup table whose content is defined by the first set of key bits.

53. (Previously Presented) The network according to claim 42, wherein said transformation circuit comprises XOR gates and controlled switches.

54. (Previously Presented) The network according to claim 53, wherein each XOR gate has two input bits and one output bit, one of the two input bits being a key bit,

and each controlled switch has two input bits, two output bits and one control bit that determines if the input bits are swapped or not, said control bit being a key bit.

55. (Previously Presented) The network according to claim 54, wherein said multiplexer circuit has two control bits, four 3-bit inputs and one 3-bit output, and said transformation circuit comprises two XOR gates and one controlled switch.

56. (Previously Presented) The network according to claim 55, wherein the three bits of said 3-bit output are connected respectively to a first input bit of each XOR gate and to the control bit of said controlled switch.

57. (Previously Presented) The network according to claim 56, wherein a second input bit of each XOR gate is connected to a bit of said second portion of said input block of bits.

58. (Previously Presented) The network according to claim 57, wherein the output bits of said XOR gates are connected to the two input bits of said controlled switch.

59. (Previously Presented) The network according to claim 58, wherein the two output bits of said controlled switch generate the transformed bits of said transformation circuit.

60. (Previously Presented) The network according to claim 42, comprising a plurality of building blocks of the same type.

61. (Previously Presented) The network according to claim 42, comprising at least two different types of building blocks.

62. (Previously Presented) The network according to claim 42, wherein adjacent layers are connected by means of a block implementing a reversible linear function.

63. (Previously Presented) The network according to claim 42, wherein two additional input and output keys having a word size equal to the first word size are bitwise XORed respectively with said input digital data and with said output digital data.

64. (Previously Presented) The network according to claim 42, wherein said first set of key bits in each layer, having a first bit size, are generated from a smaller number of secret key bits, having second bit size, by means of a key expansion algorithm.

65. (Previously Presented) The network according to claim 64, wherein said secret key bits are first expanded by means of linear transformations into said first set of key bits, using a linear code so that any subset of expanded key bits having a third bit size, are linearly independent, where the third bit size is less than or equal to the second bit size.

66. (Previously Presented) The network according to claim 65, wherein said expanded key having first bit size is used as an input to a further combinatorial key-dependent network having a of block size equal to the first bit size which is

parameterised by a fixed randomly generated key satisfying the condition that every multiplexer implements balanced binary lookup tables.

67. (Previously Presented) The network according to claim 66, wherein the expanded key having the first bit size produced after every two layers of said further combinatorial key-dependent network are used as said first set of key bits from the multiplexer circuits within the layers of the combinatorial network.

68. (Previously Presented) The network according to claim 66, wherein said further combinatorial key-dependent network comprises a plurality of layers, each layer comprising a plurality of simplified building blocks, each building block comprising:

a multiplexer having one input receiving one control bit which is passed to the output intact, for selecting one out of two key bits on a one bit output; and

a controlled switch having two input bits, two output bits and one control bit connected to the output of said multiplexer, said control bit determining if said two input bits are swapped or not.

69. (Currently Amended) A block for secret-key-controlled cryptographic functions, operating on an input block of bits for generating an output block of bits comprising:

a multiplexer circuit that receives a first portion of bits of said input block of bits and a first set of key bits as inputs, the first portion of said input block of bits operable to select a second set of key bits out of the first set of key bits, wherein the selected second set of key bits are output by said multiplexer circuit, said first portion of

bits are transferred intact without modification by an encryption operation to an output of said building block, and the number of bits in the second set of key bits is less than the number of bits in the first set of key bits; and

a transformation circuit for transforming a second portion of said input block of bits into transformed bits, according to a reversible transformation chosen, by means of said selected second set of key bits, among a plurality of reversible transformations implemented in said transformation circuit, wherein said transformation circuit transforms said second portion of said input block of bits without receiving said first portion of said input block of bits as an input and said output block of bits comprises the transformed bits followed by said first portion of said input block of bits.

70. (Previously Presented) The block according to claim 69, wherein said transformation circuit comprises XOR gates and controlled switches.

71. (Previously Presented) The block according to claim 70, wherein each XOR gate has two input bits and one output bit, one of the two input bits being a key bit, and each controlled switch has two input bits, two output bits and one control bit that determines if the input bits are swapped or not, said control bit being a key bit.

72. (Previously Presented) The block according to claim 71, wherein said multiplexer circuit has two control bits, four 3-bit inputs and one 3-bit output, and said transformation circuit comprises two XOR gates and one controlled switch.

73. (Previously Presented) The block according to claim 72, wherein the three bits of said 3-bit output are connected respectively to a first input bit of each XOR gate and to the control bit of said controlled switch.

74. (Previously Presented) The block according to claim 73, wherein a second input bit of each XOR gate is connected to a bit of said second portion of said block of bits.

75. (Previously Presented) The block according to claim 74, wherein the output bits of said XOR gates are connected to the two input bits of said controlled switch.

76. (Previously Presented) The block according to claim 75, wherein the two output bits of said controlled switch generate the transformed bits of said transformation circuit.

77. (Currently Amended) A method for encryption/decryption of input digital data having a first word size into an output digital data of the same word size, comprising;

a) dividing said input digital data into blocks of bits, each having a second word size smaller than said first word size, each block of bits being divided into a first portion and a second portion;

b) for each block of bits:

b1) receiving, at a multiplexer circuit, a first portion of said input block of bits and a first set of key bits as inputs, the first portion of said input block of

bits operating to select a second set of key bits out of the first set of key bits, wherein the selected second set of key bits are output by the multiplexer circuit, said first portion of bits are transformed intact without modification by an encryption operation to a first portion of transformed bits, and the number of bits in the second set of key [[bots]] bits is less than the number of bits in the first set of key bits;

b2) selecting, by means of said selected second set of key bits, a reversible transformation among a plurality of reversible transformations, by inputting said selected second set of key bits into a transformation circuit without also inputting said first portion of bits into said transformation circuit;

b3) applying said reversible transformation to said second portion of bits, thus generating a second portion of transformed bits;

c) collecting the transformed bits from each block into said output digital data, wherein the transformed bits from each block comprise the second portion of transformed bits followed by the first portion of transformed bits.

78. (Previously Presented) The method according to claim 77, wherein said step b) is reiterated on a block of bits comprising said first and second portions of previously transformed bits.

79. (Previously Presented) The method according to claim 78, wherein, before each reiteration of step b), a fixed bit permutation is applied to said previously transformed bits.

80. (Previously Presented) The method according to claim 78, wherein, before each reiteration of step b), a reversible linear function is applied to said previously transformed bits.

81. (Previously Presented) A data processing device comprising a central processing unit, volatile or non-volatile memory, and at least a data, instruction or address bus, comprising at least a combinatorial key-dependent network according to any one of claims 42 to 68, for encryption/decryption of digital data on said data, instruction, or address bus and/or into said memories.

82. (Previously Presented) A multimedia device for storing and playing copyright digital data comprising at least a combinatorial key-dependent network according to any one of claims 42 to 68, for encryption/decryption of said copyright digital data.